IPA Information-technology Promotion Agency, Japan

プレスリリース
第 11-28-226 号
2011 年 8 月 3 日
独立行政法人情報処理推進機構

コンピュータウイルス・不正アクセスの届出状況［2011 年 7 月分］について

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2011 年 7 月のコンピュータウイルス・不正アクセスの届出状況をまとめました。

1. 今月の呼びかけ

「 スマートフォンを安全に使おう！ 」

IPA では 2011 年 2 月にスマートフォンのウイルスに関する呼びかけ※1 を発表しましたが、その後も新しいウイルスが次々と発見されており、利用者にとってウイルス感染の脅威はますます高まってきています。

また、ここ最近の IPA のウイルス届出の状況においても、スマートフォン（特に Android 端末）を狙ったウイルスが検出され始めています。

このような状況を考慮し、今回改めてスマートフォンをとりまくウイルス事情を解説するとともに、スマートフォンを安全に使うためにとるべき具体的な手段を紹介します。

※1 IPA-2011 年 2 月の呼びかけ「スマートフォンのウイルスに注意！」
http://www.ipa.go.jp/security/txt/2011/02outline.html

図 1-1：スマートフォンがウイルスに狙われつつあるイメージ図

（1）最近のスマートフォンのウイルス事情

表 1-1 はこれまで IPA に届出のあった、Android 端末を狙ったウイルスの一覧です。

表 1-1：IPA に届出のあった、Android 端末を狙ったウイルス

届出時期	名称	特徴
2011 年 3 月	AndroidOS/Lotoor（ロトール）[DroidDream]（ドロイドドリーム）	ウェブサイトからダウンロードすることにより感染し、Android 端末に保存されている情報を収集、外部に送信するといった機能を有する。
2011 年 6 月	AndroidOS/Lightdd（ライトディーディー）	感染すると、Android 端末の情報を盗み取り、外部に送信する。
2011 年 6 月	AndroidOS/Smspacem（エスエムエスパーセム）	感染すると、Android 端末内のアドレス帳の連絡先に、SMS※2 メッセージの送信を試みる。
2011 年 6 月	AndroidOS/Smstibook（エスエムエスティブック）	感染すると、事前に設定された番号に、プレミアム SMS※3 メッセージの送信を試みる。

※2 SMS（Short Message Service）：携帯電話同士で、短い文章のメールを送受信できるサービス。
※3 プレミアム SMS：発信者がメッセージを送るだけで、相手先が利益を得る仕組みが付加された SMS。

このように、今年に入ってからスマートフォンを狙ったウイルスが次々と発見されており、利用者にとってウイルス感染の脅威がますます高まってきています。
また、スマートフォンがウイルスに感染してしまった場合に想定される被害例として、以下が考えられます。

- スマートフォン内データ、GPS※4による位置情報等、個人情報を含む重要な情報が悪意ある第三者に送られてしまう。
- 悪意ある第三者にスマートフォンを乗っ取られて、自由自在に操られてしまう。
- スマートフォンがボットネット※5の1つとして組み込まれ、知らぬ間に特定の組織にサイバー攻撃を行うなどの犯罪の道具として使われてしまう。

※4 GPS（Global Positioning System）：人工衛星の電波を使って、受信者の地球上の位置を割り出すシステムのこと。
※5 ボットネット：攻撃者が、ボットと呼ばれるウイルスに感染させた多くのコンピュータを使って、ターゲットに対し遠隔で攻撃を行うために構築されたネットワークのこと。

（2）IPA に届出のあったスマートフォンのウイルスについて

図 1-2 は 2011 年 3 月～2011 年 7 月に、IPA に届出のあったスマートフォンのウイルスの検出数のグラフです。
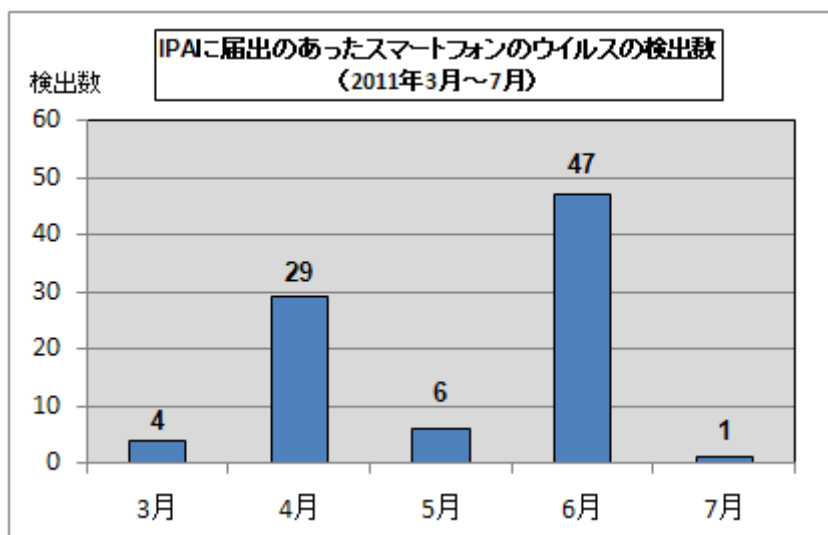
図 1-2：IPA に届けられたスマートフォンのウイルスの検出数（2011 年 3 月～7 月）

これらのウイルスは全て、スマートフォン上で発見されたものではなく、Windows などパソコンの環境でメール受信時などに検出されたものでした。メールにウイルスを添付して、それをスマートフォン上で開かせることでウイルス感染させようという意図から、メールが不特定多数に送られたため、パソコンにも届いているようです。加えて、Android 端末用のセキュリティソフトがあまり普及していないために、スマートフォン上でのウイルス発見の報告がまだないものと思われます。なお、2011 年 3 月から 7 月に届出のあったスマートフォンのウイルスは、全て Android 端末をターゲットとするものでした。

ウイルスが混入したアプリが添付されたメールをスマートフォンで受信した場合、スマートフォンの機種やOSによっても挙動が異なりますが、特に**Android端末の場合はメール表示中の「インストール」ボタンを押すとアプリのインストールが開始され、ウイルスに感染してしまう場合がある**ため、取り扱いには十分注意する必要があります。図 1-3 は、Android アプリ（.apk ファイル）が添付されたメールをスマートフォン（端末名：GALAXY Tab/OS バージョン：Android 2.2）上で見た際の画面例です。
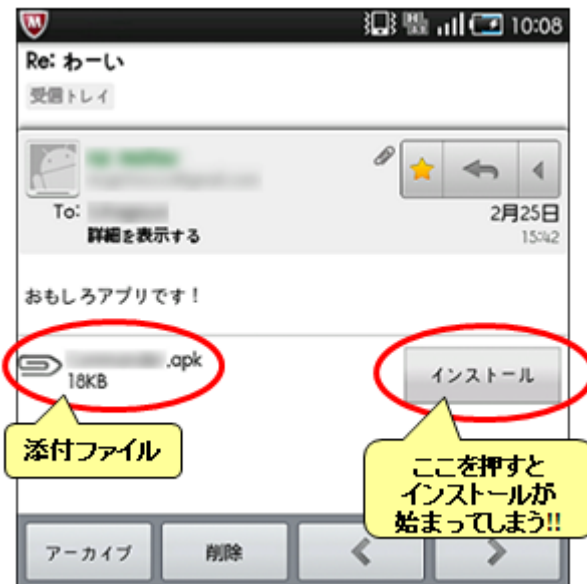
図 1-3：Android アプリが添付されたメールをスマートフォン上で見た画面例

（3）スマートフォンを安全に使用するための六箇条

上述したようなスマートフォンに関するウイルスの現状を受け、IPA では特にウイルスと脆弱（ぜいじゃく）性を悪用した攻撃への対策を考慮した、スマートフォンを安全に使用するための六箇条をまとめましたので、スマートフォン使用時の指針としてください（図 1-4 参照）。

1. スマートフォンをアップデートする。
2. スマートフォンにおける改造行為を行わない。
3. 信頼できる場所からアプリケーション（アプリ）をインストールする。
4. アンドロイド端末では、アプリをインストールする前に、アクセス許可を確認する。
5. セキュリティソフトを導入する。
6. スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

図 1-4：スマートフォンを安全に使用するための六箇条

各項目について以下に詳しく説明します。

【1】スマートフォンをアップデートする。

販売元から OS のアップデートが提供された場合、早めにアップデートしましょう。アップデートをしないで使っていると、パソコン同様、脆弱性を悪用した攻撃に遭う危険性が高まります。またその際、アップデート手順をきちんと理解することが重要です。アップデート手順は、販売元や製造元によって異なる場合があります。きちんとアップデートするために、取扱説明書などを確認し、正しい手順を身につけたうえでアップデートを実践しましょう。

【2】スマートフォンにおける改造行為を行わない。

スマートフォンにおける改造行為はやめましょう。ここでの改造行為とは、いわゆる iPhone における Jailbreak（脱獄）や Android 端末における root 権限奪取行為（root 化とも呼ばれる）などのことを指します。スマートフォンで動作するウイルスの中には、改造行為を行ったスマートフォンのみに感染するものも確認されています。ウイルス感染の危険性を自ら高めてしまうことになりますので、スマートフォンの改造行為はやめましょう。

【3】信頼できる場所からアプリケーション（アプリ）をインストールする。

スマートフォンで使用するアプリは、iPhone であれば米 Apple 社の「App Store」、Android 端末であればアプリの審査や不正アプリの排除を実施している場所（米 Google 社の「Android Market」）など信頼できる場所からインストールしましょう。

【4】Android 端末では、アプリをインストールする前に、アクセス許可を確認する。

Android 端末の場合、アプリをインストールする際に表示される「アクセス許可」（アプリが Android 端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう（図 1-5 参照）。過去発見された Android 端末を狙ったウイルスには、個人情報などを不正に盗み取るため、アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。例としては、壁紙アプリにも関わらず、アドレス帳の内容や通話履歴の記録へアクセスするための「連絡先データを読み取り」の許可を求めるなどといったものがあります。Android 端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止しましょう。

図 1-5：「アクセス許可」の表示画面の例

【5】セキュリティソフトを導入する。

スマートフォンの中でも Android 端末では、2011 年初頭以降大手ウイルス対策ソフトベンダーが続々とセキュリティソフトを発売し、その選択肢が充実してきました。Android 端末では **【4】** に注意すればウイルスに感染する可能性を低減できますが、ゼロにはできません。ウイルス感染の可能性をより低減するためにセキュリティソフトを導入してください。

【6】スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

企業でスマートフォンを活用する場合、スマートフォンの利用ルール、スマートフォンからアクセス可能な情報の範囲、スマートフォンに保存してよい情報の範囲、紛失・盗難時の対応等のポリシーを定めましょう。特に端末管理（MDM：Mobile Device Management）によって、スマートフォンに搭載されている OS のアップデートの徹底やインストールできるアプリの制限等を企業側が強制的に管理できる仕組みを設けることをおすすめします。

今月のトピックス

○ コンピュータ不正アクセス被害の主な事例（届出状況および被害事例の詳細は、7 頁の「3.コンピュータ不正アクセス届出状況」を参照）

・サーバーの設定不備を突かれて侵入され、ファイルを置かれた
・ファイアウォールに見知らぬルールが追加されていた

○ 相談の主な事例 （相談受付状況および相談事例の詳細は、9 頁の「4.相談受付状況」を参照）
・iPad でアダルトサイトにアクセスしたら、当該サイトの画面が消えなくなった
・IPA と間違えて別の組織にワンクリック請求の対処を依頼してしまった

○ インターネット定点観測（11 頁参照。詳細は、別紙 3 を参照）
IPA で行っているインターネット定点観測について、詳細な解説を行っています。

2. コンピュータウイルス届出状況 ―詳細は別紙 1 を参照―

（1）ウイルス届出状況

7 月のウイルスの検出数※1 は、**約 2.3 万個**と、6 月の約 3.8 万個から 39.4%の減少となりました。また、7 月の届出件数※2 は、**1,064 件**となり、6 月の 1,209 件から 12.0%の減少となりました。

※1 検出数 ：届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数：同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1 日何個検出されても届出 1 件としてカウントしたもの。
・7 月は、寄せられたウイルス検出数約 2.3 万個を集約した結果、1,064 件の届出件数となっています。

検出数の 1 位は、**W32/Netsky** で**約 1.0 万個**、2 位は **W32/Mydoom** で**約 9.5 千個**、3 位は **W32/Autorun** で**約 1.5 千個**でした。
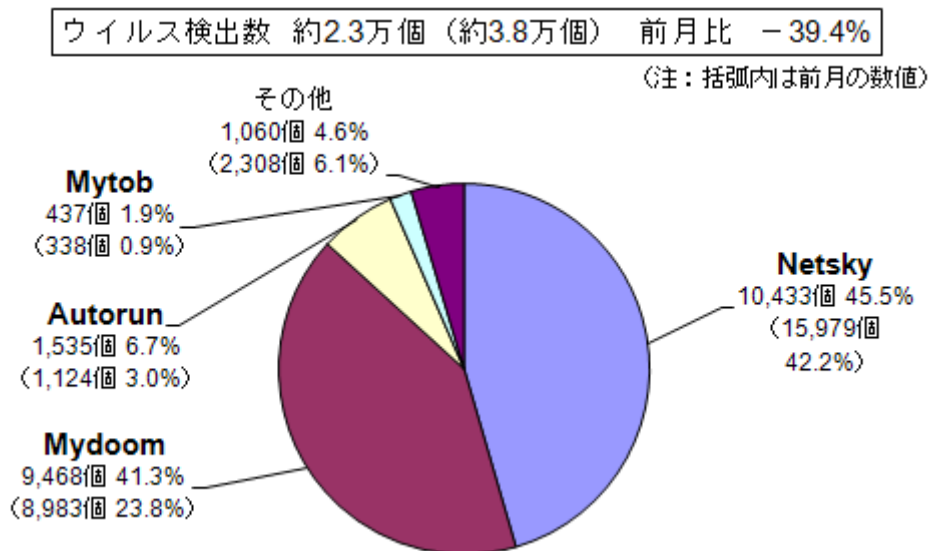
図 2-1：ウイルス検出数
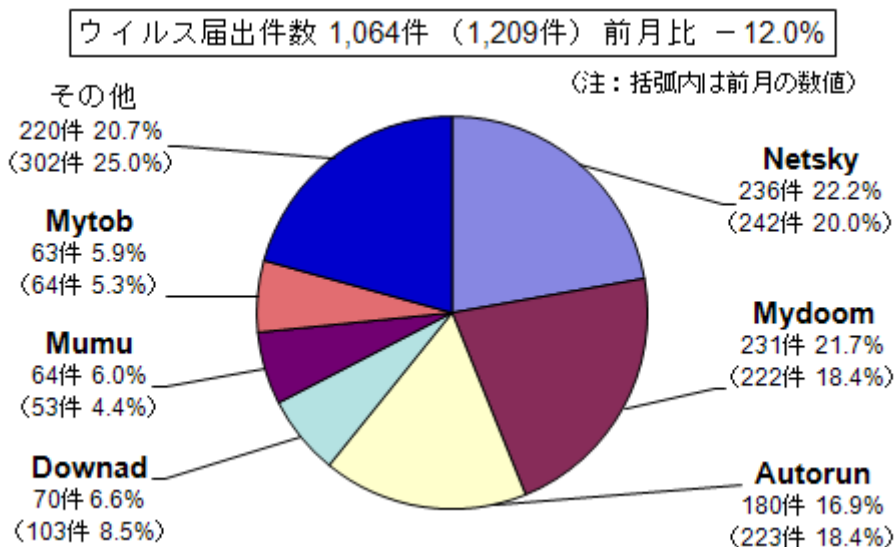
図 2-2：ウイルス届出件数

（2）不正プログラムの検知状況

7 月は、特に目立った動きはありませんでした（図 2-3 参照）。
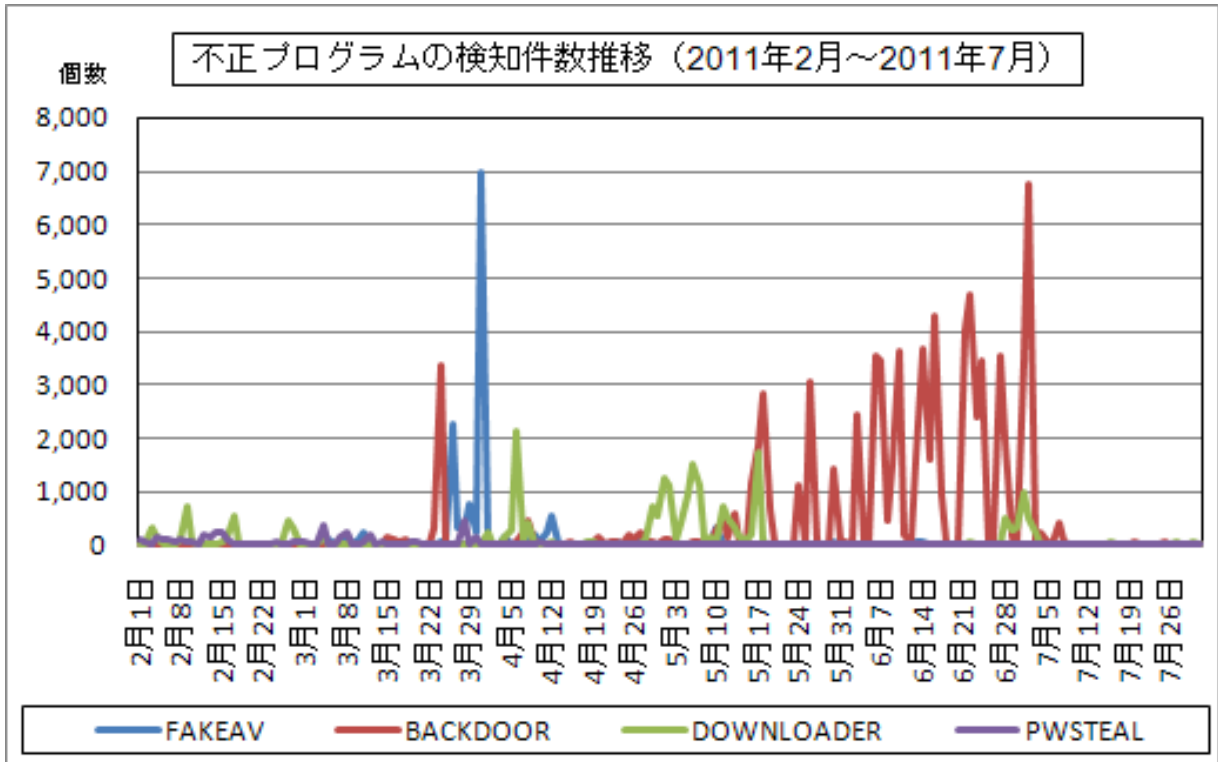
図 2-3：不正プログラムの検知件数推移

3. コンピュータ不正アクセス届出状況（相談を含む）　－詳細は別紙 2 を参照－

表 3-1　不正アクセスの届出および相談の受付状況

	2月	3月	4月	5月	6月	7月
届出[a] 計	10	6	5	7	9	8
被害あり[b]	5	6	5	6	9	5
被害なし[c]	5	0	0	1	0	3
相談[d] 計	23	45	38	55	32	47
被害あり[e]	6	10	10	14	7	15
被害なし[f]	17	35	28	41	25	32
合計[a+d]	33	51	43	62	41	55
被害あり[b+e]	11	16	15	20	16	20
被害なし[c+f]	22	35	28	42	25	35

(1) 不正アクセス届出状況

7 月の届出件数は 8 件であり、そのうち何らかの被害のあったものは 5 件でした。

(2) 不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は 47 件であり､そのうち何らかの被害のあった件数は 15 件でした。

(3) 被害状況

被害届出の内訳は、**侵入 4 件、なりすまし 1 件**でした。

「侵入」の被害は、データベースから設定情報が盗まれたものが 1 件、外部サイトを攻撃するツールを埋め込まれ、踏み台として悪用されていたものが 2 件、ファイルを勝手にアップロードされていたものが 1 件でした。侵入の原因は、設定不備が 3 件（アクセス制限の設定不備が 2 件、普段使用していない機能が有効になっていてその機能を使われたものが 1 件）で、他は原因不明でした。

「なりすまし」の被害は、本人になりすまして何者かにログインされ、IP 電話サービスを勝手に利用されていたものが 1 件、でした。

（4）被害事例

［侵入］

（i）サーバーの設定不備を突かれて侵入され、ファイルを置かれた

事例	・組織外から「ウェブサーバーに対するアップロードの通信を検知した」との連絡が入った。 ・調査したところ、当該サーバーのウェブアプリケーション格納ディレクトリに、見知らぬファイルを発見。 ・当該サーバーでは Tomcat を使用しており、Tomcat のウェブアプリケーションマネージャ機能が有効になっていた。その機能を使用してファイルをサーバー上にアップロードされていた。 ・事後対策として、Tomcat のウェブアプリケーションマネージャ機能は不要であると判断したため、削除した。
解説・対策	使われていない機能が設定不備のまま放置されていたことが原因でした。 Tomcat のウェブアプリケーションマネージャは、ネットワーク経由でウェブアプリケーションを配備できるので便利な一方、悪用されると不正なファイルのアップロードに使用されてしまいます。同機能が不要の場合は機能の削除を、必要の場合は専用アカウントを作成した上で（パスワードは強固なものを使用して）運用することを勧めます。 一般的に、使われていない機能やサービスは管理や監視の対象から外れることになるため、セキュリティ対策漏れにつながります。当初は必要だった機能でも、現在は不要になっている可能性があります。**サーバーで動作させる機能やサービスの棚卸し**を、定期的に実施することをお勧めします。 （ご参考） IPA-安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

［不正プログラム埋め込み］

（ii）ファイアウォールに見知らぬルールが追加されていた

事例	・社内規程に反するファイアウォールの設定を発見した。社内のあるサーバーに対して全ての通信を許可するルールになっていた。 ・当該サーバーを調査した結果、当該サーバーに不正なプログラムを埋め込まれて外部への SSH スキャンの踏み台にされていた。 ・事後対策として、ファイアウォールの管理用パスワードを変更するとともに、ファイアウォール変更申請手続の実施を徹底するために実施方法の見直しを行った。 ・現在調査中だが内部犯行の可能性がある。
解説・対策	いくら社内文書で規定していても、技術的に可能な限り、社員による不正アクセスの脅威は常に存在します。対策の一環として、ファイアウォールを含めたネットワーク機器、および各種サーバーの**管理用パスワードは強固なもの**にしてください。また共用のアカウントではなく、**担当者ごとに個別のアカウントを発行**し、有事の際に追跡可能にしておくことも重要です。 各種アクセスログの取得も必須ですが、そのことを社内にアナウンスすることで、社内犯行の抑止力になる場合があります。 （ご参考） IPA-情報セキュリティガバナンス http://www.ipa.go.jp/security/manager/know/meaning/governance.html

4. 相談受付状況

7 月のウイルス・不正アクセス関連相談総件数は **1,490 件**でした。そのうち**『ワンクリック請求』に関する相談が** **461 件**（6 月：511 件）、**『偽セキュリティソフト』**に関する相談が **8 件**（6 月：11 件）、**Winny に関連する相談が** **7 件**（6 月：7 件）、**「情報詐取を目的として特定の組織に送られる不審なメール」に関する相談が** **2 件**（6 月：6 件）、などでした。

表 4-1 IPA で受け付けた全てのウイルス・不正アクセス関連相談件数の推移

		2月	3月	4月	5月	6月	7月
合計		1,521	1,723	1,608	1,640	1,692	1,490
	自動応答システム	892	1,106	997	950	999	889
	電話	570	551	555	620	639	540
	電子メール	53	58	50	62	50	54
	その他	6	8	6	8	4	7

※ IPA では、「情報セキュリティ安心相談窓口」を開設し、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。
メール：anshin@ipa.go.jp
電話番号：03-5978-7509 （24 時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金の 10:00～12:00、13:30～17:00 のみ）
FAX：03-5978-7518 （24 時間受付）

※ 「自動応答システム」：電話の自動音声による応対件数
「電話」：IPA セキュリティセンター員による応対件数

※ 合計件数には、「不正アクセスの届出および相談の受付状況」における『相談（d）計』件数を内数として含みます。
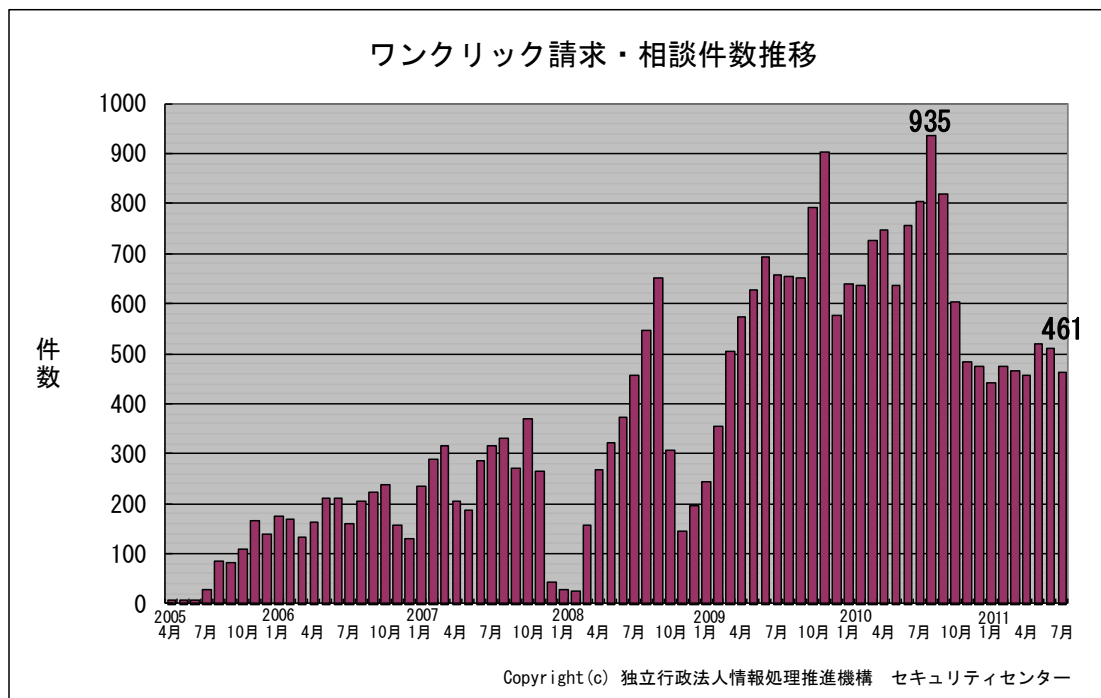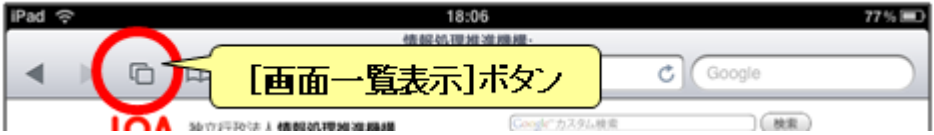
図 4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

（i）iPad でアダルトサイトにアクセスしたら、当該サイトの画面が消えなくなった

相談	iPad でアダルトサイトにアクセスしたら、当該サイトのページが張り付いた状態で消えなくなり、iPad を再起動しても残ったままになっている。 これはパソコンでいうところのワンクリック請求の症状が、iPad で起きているということか。iPad の場合はどうやって画面を消せばいいのか。
回答	この場合、**iPad のブラウザである Safari のキャッシュや履歴として当該ページの情報が残っているために、Safari を開くたびにその情報を読み込んでしまい、画面が張り付いているように見えている**ということでしょう。**Safari で［画面一覧表示］ボタンを押し、閉じたい画面の左上にある（X）を押すことで、再び画面が出てくる状況を解消することができます。** 図 4-2：iPad の Safari の画面上部 iPad 上で請求画面を出すワンクリック請求の事例は、IPA ではまだ確認していませんが、今後 iPad でも同様の現象が起こりうる可能性は否定できませんので、ウェブサイトへのアクセスには十分注意してください。 （ご参考） IPA-「【注意喚起】ワンクリック請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！」 http://www.ipa.go.jp/security/topics/alert20080909.html

（ii）IPA と間違えて別の組織にワンクリック請求の対処を依頼してしまった

相談	パソコン上にアダルトサイトの請求画面が張りついて消えなくなった。 消費生活センターに相談したところ、請求画面を削除する方法については、IPA のウェブサイトを参照するように案内されたので、検索サイトで“IPA”を検索して、検索結果の上位に表示された組織の URL を IPA と思い込んでアクセスした。有料のサービスだったが電話対応してくれそうだったので、指示に従い請求画面を削除することができた。しかし、改めて当該組織のウェブサイトを確認してみたところ、IPA ではなかったことに気付いた。 IPA で検索したはずなのに、一体どういうことなのか。
回答	**あなたが対処を依頼した組織は、IPA とは無関係の別の組織です。** **検索サイトでキーワード検索を行う際、必ずしも目的の情報が上位に表示されるとは限りません。**また、検索サイトによっては、検索結果より上位に広告スポンサーの情報が表示される場合があります。 **検索サイトで目的の情報を探す場合、検索結果に表示されるタイトル、URL、説明書きなどを十分確認し、間違った情報にアクセスしないようにしてください。** なお、IPA が公開しているワンクリック請求に関する情報については、以下のページを参照ください。 （ご参考） IPA-「【注意喚起】ワンクリック請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！」 http://www.ipa.go.jp/security/topics/alert20080909.html

5. インターネット定点観測での 7 月のアクセス状況

インターネット定点観測（TALOT2）によると、2011 年 7 月の期待しない（一方的な）アクセスの総数は 10 観測点で **102,888 件**、延べ発信元数※は **46,222 箇所**ありました。平均すると、**1 観測点につき 1 日あたり 154 の発信元から 343 件のアクセスがあった**ことになります（図 5-1 参照）。

延べ発信元数※：TALOT2 の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合は、発信元数を 1 としてカウントする。

TALOT2 における各観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。

※7 月 2 日は保守作業のため、システムを停止しています。そのため、7 月の観測データは、この 1 日を除外して統計情報を作成しています。なお、通常は常時稼動しています。
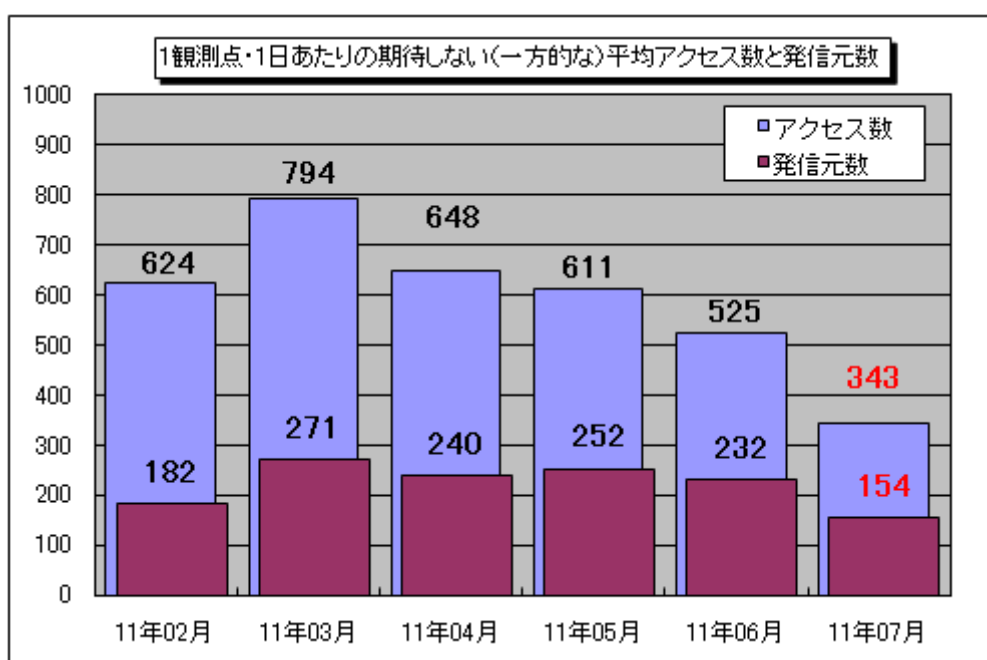
図 5-1：1 観測点・1 日あたりの期待しない（一方的な）平均アクセス数と発信元数

2011 年 2 月～2011 年 7 月までの各月の 1 観測点・1 日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図 5-1 に示します。7 月の期待しない（一方的な）アクセスは、6 月と比べて大きく減少しました。

6 月と 7 月の宛先（ポート種類）別アクセス数の比較を図 5-2 に示します。445/tcp が大きく減少したにもかかわらず、増加が観測されたのは 11083/tcp からのアクセスでした。
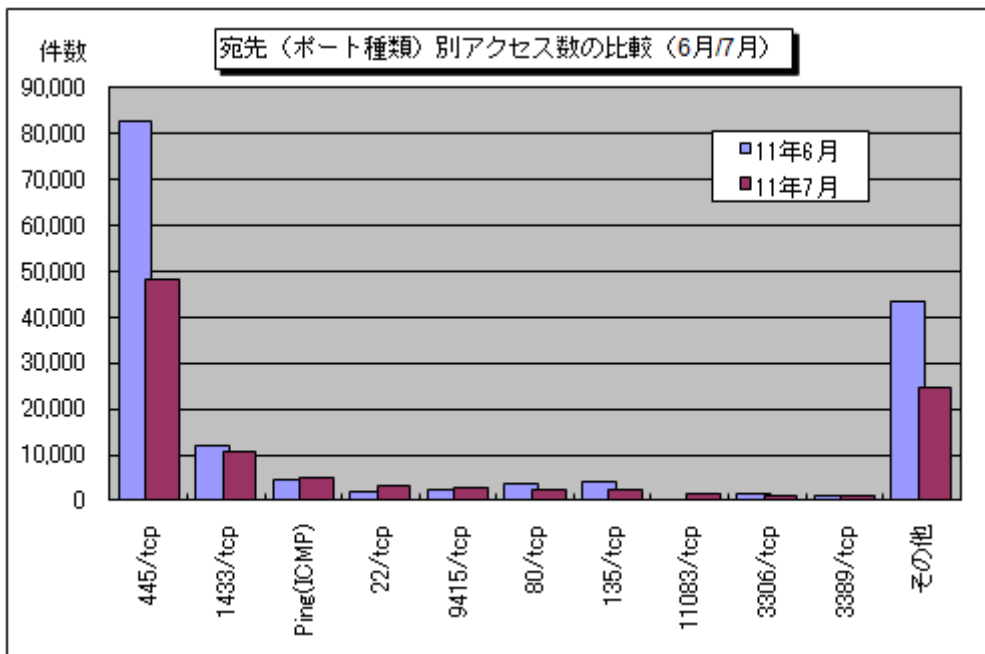
図 5-2：宛先（ポート種類）別アクセス数の比較（6 月/7 月）

11083/tcp は、7 月 3 日以降に TALOT2 の特定の 1 観測点で観測され始めたアクセスであり、発信元地域はアメリカと中国が大部分を占めていました（図 5-3 参照）。このポートは特定のアプリケーションで使用されるポートというわけではなく、このアクセスが何を目的としたものだったかは不明です。
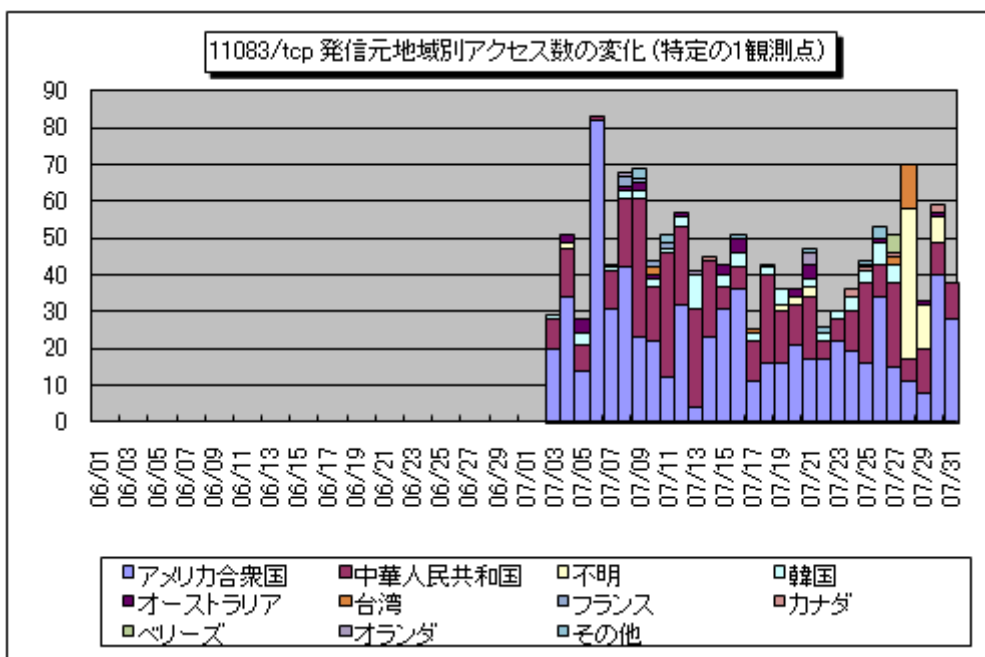
図 5-3：11083/tcp 発信元地域別アクセス数の変化（特定の 1 観測点）

以上の情報に関して、詳細はこちらをご参照ください。
別紙 3_インターネット定点観測（TALOT2）での観測状況について
http://www.ipa.go.jp/security/txt/2011/documents/TALOT2-1108.pdf

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』

一般社団法人 JPCERT コーディネーションセンター：http://www.jpcert.or.jp/
@police：http://www.cyberpolice.go.jp/
フィッシング対策協議会：http://www.antiphishing.jp/
株式会社シマンテック：http://www.symantec.com/ja/jp/
トレンドマイクロ株式会社：http://www.trendmicro.com/jp/
マカフィー株式会社：http://www.mcafee.com/japan/